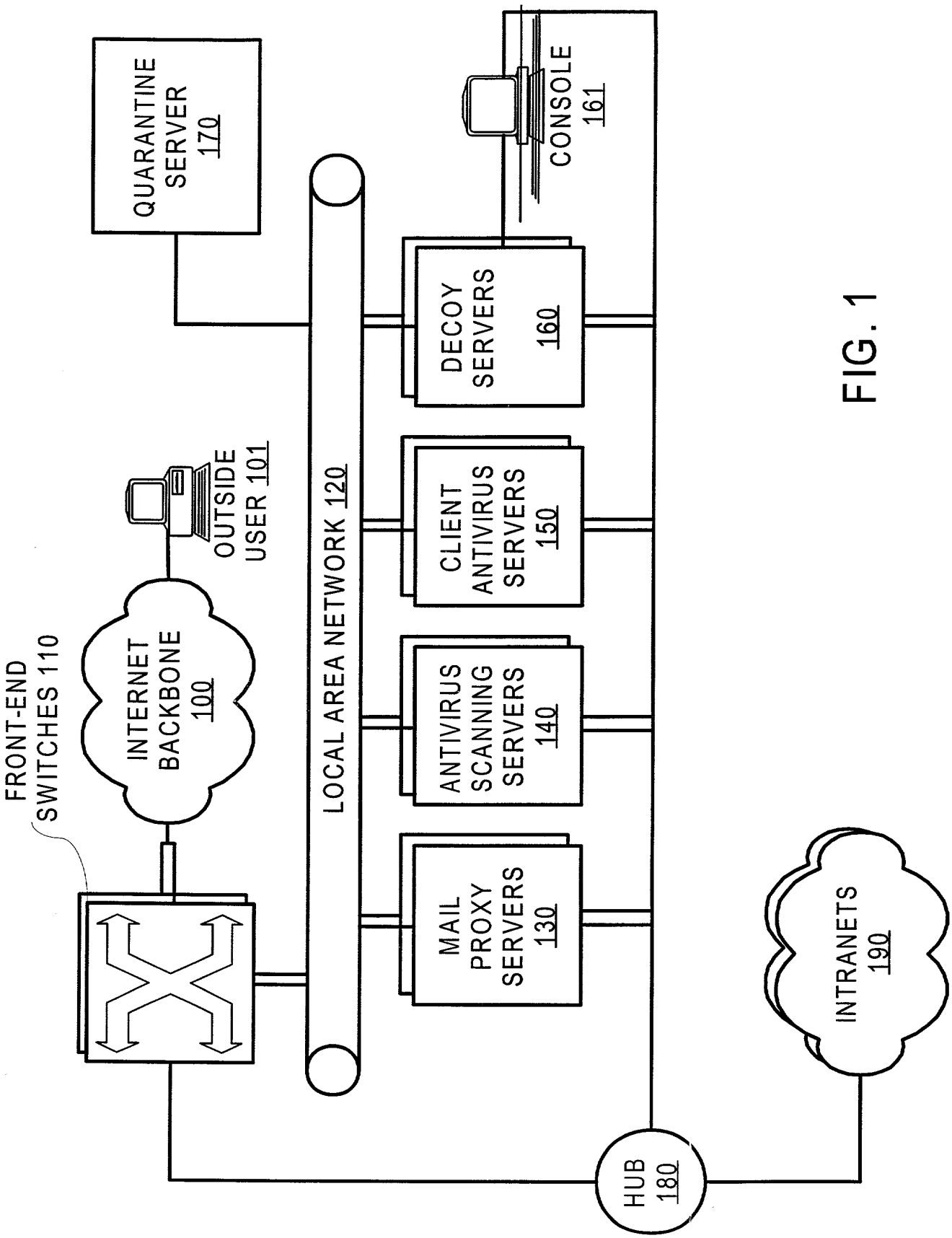
QUARANTINE SERVER 170
CONSOLE 161
DECOY SERVERS 160
CLIENT ANTIVIRUS SERVERS 150
ANTIVIRUS SCANNING SERVERS 140
MAIL PROXY SERVERS 130
OUTSIDE USER 101
INTERNET BACKBONE 100
FRONT-END SWITCHES 110
LOCAL AREA NETWORK 120
INTRANETS 190
HUB 180

FIG. 1

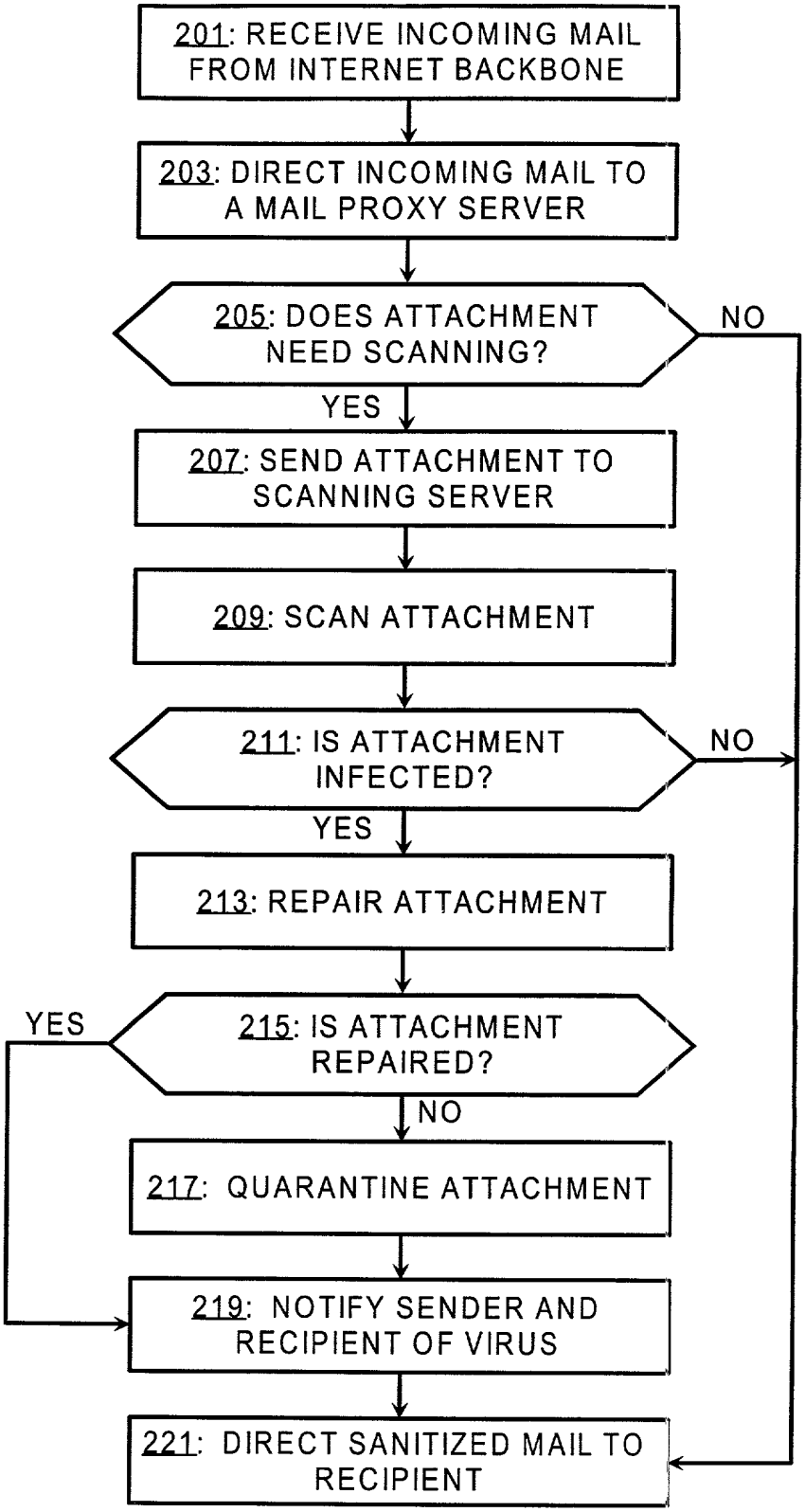
201: RECEIVE INCOMING MAIL FROM INTERNET BACKBONE
203: DIRECT INCOMING MAIL TO A MAIL PROXY SERVER
205: DOES ATTACHMENT NEED SCANNING?
NO
YES
207: SEND ATTACHMENT TO SCANNING SERVER
209: SCAN ATTACHMENT
211: IS ATTACHMENT INFECTED?
NO
YES
213: REPAIR ATTACHMENT
YES
215: IS ATTACHMENT REPAIRED?
NO
217: QUARANTINE ATTACHMENT
219: NOTIFY SENDER AND RECIPIENT OF VIRUS
221: DIRECT SANITIZED MAIL TO RECIPIENT

FIG. 2

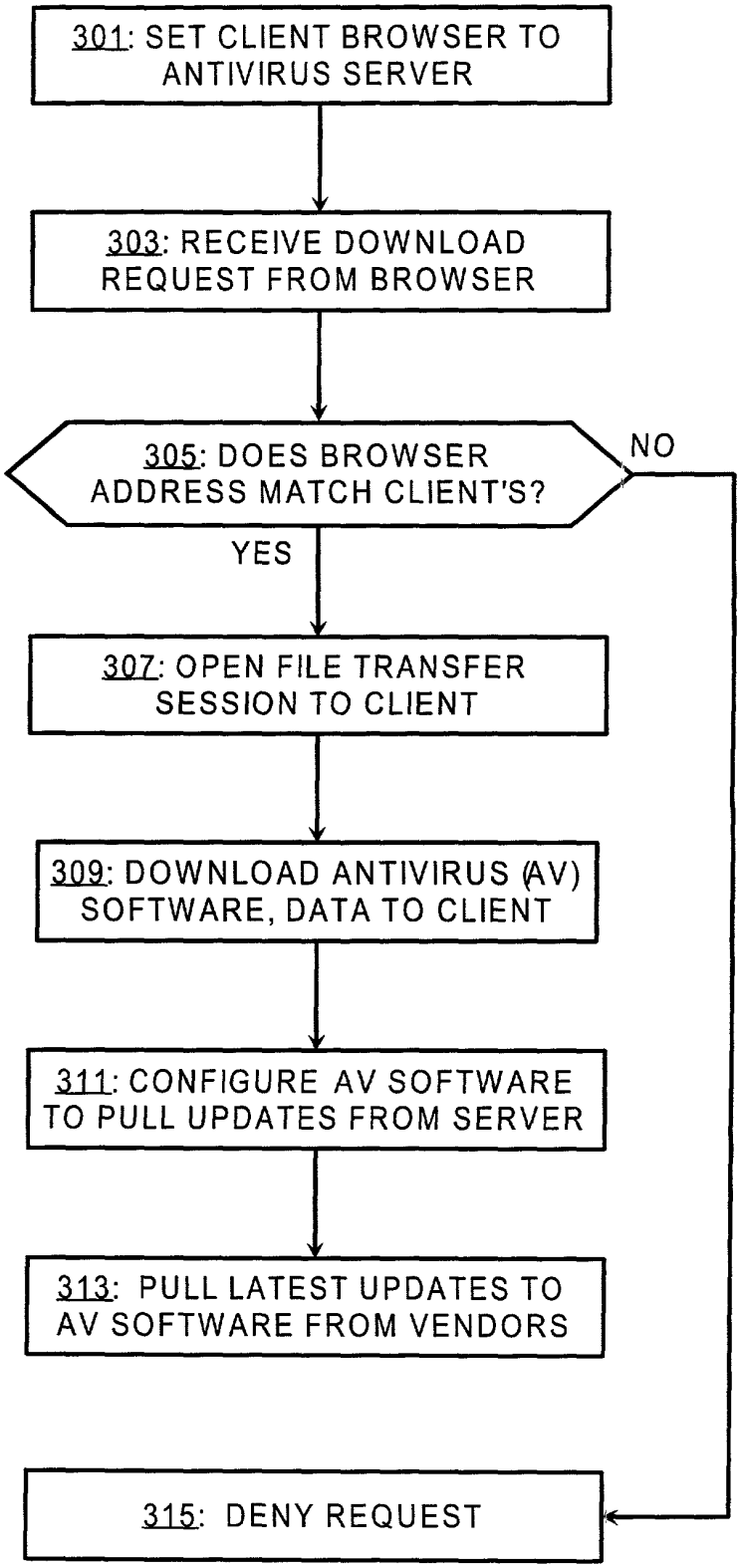
301: SET CLIENT BROWSER TO ANTIVIRUS SERVER
303: RECEIVE DOWNLOAD REQUEST FROM BROWSER
305: DOES BROWSER ADDRESS MATCH CLIENT'S?
NO
YES
307: OPEN FILE TRANSFER SESSION TO CLIENT
309: DOWNLOAD ANTIVIRUS (AV) SOFTWARE, DATA TO CLIENT
311: CONFIGURE AV SOFTWARE TO PULL UPDATES FROM SERVER
313: PULL LATEST UPDATES TO AV SOFTWARE FROM VENDORS
315: DENY REQUEST

FIG. 3

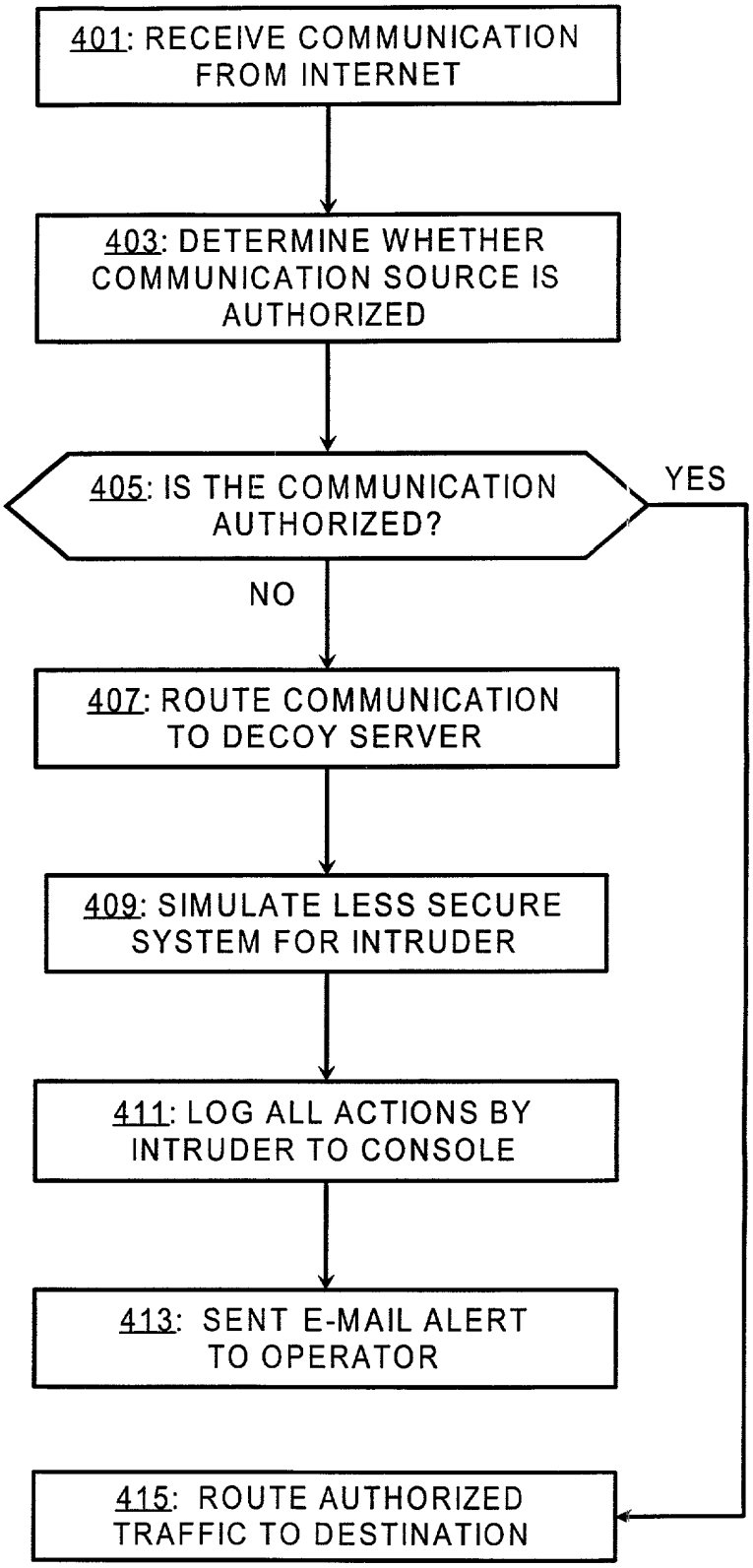
401: RECEIVE COMMUNICATION FROM INTERNET
403: DETERMINE WHETHER COMMUNICATION SOURCE IS AUTHORIZED
405: IS THE COMMUNICATION AUTHORIZED?
YES
NO
407: ROUTE COMMUNICATION TO DECOY SERVER
409: SIMULATE LESS SECURE SYSTEM FOR INTRUDER
411: LOG ALL ACTIONS BY INTRUDER TO CONSOLE
413: SENT E-MAIL ALERT TO OPERATOR
415: ROUTE AUTHORIZED TRAFFIC TO DESTINATION

FIG. 4

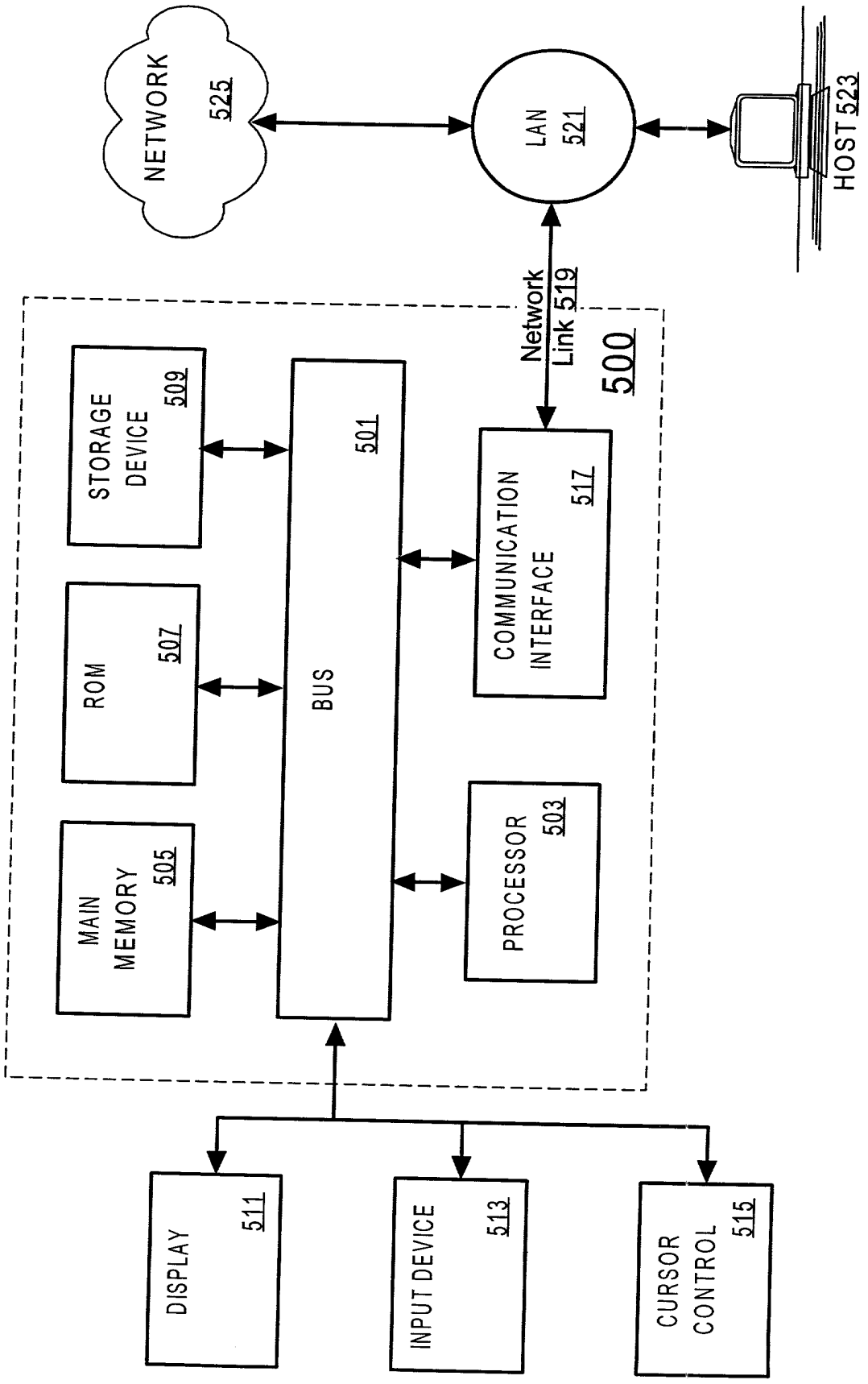
NETWORK
525
LAN
521
HOST 523
Network
Link 519
500
STORAGE
DEVICE
509
ROM
507
MAIN
MEMORY
505
BUS
501
COMMUNICATION
INTERFACE
517
PROCESSOR
503
DISPLAY
511
INPUT DEVICE
513
CURSOR
CONTROL
515

FIG. 5